IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
vs.	)	**Cr. No. 05-344**
	)	
ARTHUR ABRAHAM	)	

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Defendant Arthur Abraham has been charged in a one-count Indictment with distributing child pornography in violation of 18 U.S.C. §2552(a)(2). Specifically, the Indictment against Defendant charges:

> On or about February 28, 2005, in the Western District of Pennsylvania and elsewhere, the defendant, ARTHUR ABRAHAM, did knowingly distribute, by computer, a visual depiction of a minor, the production of which involved the use of a minor engaging in sexually explicit conduct, and which depicted a minor engaging in sexually explicit conduct, as those terms are defined in Title 18, United States Code, Section 2256, which had been shipped and transported in interstate and foreign commerce and which contains materials which have been mailed and shipped and transported in interstate and foreign commerce.

> In violation of Title 18, United States Code, Section 2252(a)(2).

The defendant stipulated that the movie image in question depicts a minor engaged in sexually explicit conduct. Stipulation of Fact and Authenticity, ¶ 3. Defendant waived his right to a jury trial and on June 26, 2006, this Court held a one-day bench trial. The issue here is whether or not a Pennsylvania state trooper's downloading of a movie file containing child pornography from the defendant's computer as a result of the defendant's installation of an internet peer-to-peer video file sharing program constitutes knowing distribution by computer of a visual depiction of a minor, the production of which involved the use of a minor engaging in sexually explicit conduct. Both sides have timely submitted briefs.

Pursuant to Federal Rule of Criminal Procedure 23(c), after presiding over the trial and carefully reviewing the trial transcript, exhibits, and briefs, the Court hereby enters the following findings of fact and conclusions of law based upon consideration of all the admissible evidence as well as this Court's own assessment of the credibility of the trial witnesses.

I. The Court's Findings of Fact.

A. Facts relevant to how peer to peer filing sharing works.

The facts relevant to this case began on February 28, 2005, when at 4:35 p.m., Trooper Robert Erderly of the Pennsylvania State Police was logged onto a computer located at the Pennsylvania State Police barracks in Indiana, Pennsylvania. Trial transcript ("TT.") 18-19.

Installed on the computer used by Trooper Erdely on February 28, 2005, was a file-sharing software program called Phex. TT. 13. Trooper Erdely used the Phex program to search for files on the Gnutella network. TT. 13-14. BearShare and LimeWire are other such file-sharing software programs. TT. 14. With a peer-to-peer file-sharing network, the files come from the individual clients. TT. 29.

How the Phex file-sharing program works is that the user types in a search term in a field that is provided for the user; the user then submits that search. TT. 14. The Phex program searches all the computers on the Gnutella network that are also running a file-sharing program. This enables the user to see who has files that have been selected to be shared with others that have similar names to the search term which the user has inputted into the program. TT. 15. Once the Gnutella network is searched, the user gets a list of persons offering files that are similar in name to the terms the user used in the search. TT. 18. At that

point, the user can choose any of those files and download that file from the computer of the person offering the file. TT. 18. The user simply clicks on the file he'd like to download and it is downloaded onto the user's computer. TT. 15.

The Gnutella network, BearShare, Phex and LimeWire share all types of files, including music, movie, photograph/still image, and text files. TT. 17. Basically, with the installation of a peer-to-peer file sharing program, any file that a person may have on his computer, can be dropped into his shared folder, and it may then be shared worldwide over the Internet. TT. 17.

On February 28 2005, the defendant, Arthur Abraham, was logged on to his computer at his residence at 3129 West Queen Lane, Philadelphia, Pennsylvania, and running a peer-to-peer file-sharing program called BearShare, version 4.6.3. TT. 25, 27. Like Phex, BearShare also uses the Gnutella Network. TT. 15. In order to use this version of BearShare, the defendant had to execute the setup program file, a file available to download for free from the Internet. TT. 27. To get the program, a person simply needs to go to www.bearshare[.com]. TT. 27. The available version is downloaded onto the user's computer by clicking on a link. TT. 27. It will copy a file over the Internet onto the computer. TT. 27. Then to execute the program and so begin installation of the file sharing program, one just double clicks on that copied file. TT. 27. Next, the user selects the run option and the program will begin to install. TT. 28. The program provides a description of what the program is about. TT. 28. The program states that "BearShare is the premiere peer to peer program which allows you to connect directly to fellow users without any type of centralized server. BearShare has search on demand, easy to use downloading capabilities and highly customizable sharing features." TT. 28.

3

Once BearShare is installed, any file a person chooses to share is available to anyone on the Gnutella network. TT. 29. Every computer that is running this Gnutella network can participate in the sharing of the files. TT. 29.

In order to install the version of the BearShare program that the defendant had on his computer on February 28, 2005, the defendant had to have accepted the terms of an end user software licensing agreement. TT. 30. With this agreement, the user acknowledges that he is using a file sharing program which can be used both to download files and to send files out over the Internet, i.e. share files. TT. 30. The agreement states that the user should not share child pornography. TT. 30.

After the user accepts the terms of the end user software licensing agreement, BearShare's installation program next asks the user where he wants to install the program on his computer. TT. 31. The program will pop up with the default location which is on the user's hard drive at c:\. TT. 31. The installation program will create a directory called "BearShare." TT. 31. The user must select where he wants the BearShare program to be installed on his computer; otherwise the program won't run. TT. 32.

At this point, the BearShare program thanks the user "for using BearShare as your preferred file sharing application." Exhibit 5, unnumbered page 10. Once the BearShare program is installed on the user's computer, there is a "finish" button. TT. 33. The user is then given a link to the user's guide where the user can find out every single option within the BearShare program, what the user can use and not use and how to effectively run the program. TT. 33. Basically, it is the instruction manual. TT. 33. Then, the program asks the user if the user want to run BearShare now. TT. 33.

Importantly, the first time the BearShare program is run on a computer, the program starts the user in a setup wizard; a setup wizard is a walk through, step-by-step process to further define different aspects of the program for the user. TT. 34. The user first selects yes, he wants to run the BearShare program. TT. 34. Then a screen appears that says in relevant part "Welcome to the Bearshare Setup Wizard! This Wizard will guide you through the steps necessary to configure your software to operate efficiently on the Internet. . . ." TT. 34. This wizard only appears (1) the first time the program is run, (2) when a person removes the settings file or (3) if a newer version requires additional information. TT. 34, Exhibit 5, unnumbered page 15.

The set-up wizard then gives a number of options. TT. 34. One option, which by default is checked, i.e. selected, is the ability to launch the BearShare program on system startup. TT. 34, Exhibit 5, unnumbered page 16. This means that if the user is automatically connected to the Internet, as soon as the user turns on his computer, the BearShare program will begin to run and be sharing over the Internet all of the files the user has chosen to share. TT. 34. The user has the option to deselect any of these options. TT. 34.

With the Bearshare set-up wizard, the user next selects the type of network being used (modem or dsl or satellite, etc.). TT. 35. The user is then asked where he wants incomplete and completed downloaded files be saved. TT. 35. The default for when an item is completely downloaded is in the c:\ drive, in a folder called "My Downloads." TT. 35. This option can be changed and the user could have the completely downloaded file located wherever he'd like on the computer. TT. 35.

The set-up wizard next states that "the wizard will search your computer for folders containing files that you can then choose to make accessible to other Bearshare users. Please

select the drive(s) you would like to search from the list on the right." Exhibit 5, unnumbered page 19. In other words, the program allows a user to search his hard drive for files he'd like to share. TT. 36. The user simply clicks on the drive he'd like to search for files such as music files or movie files, or any other file the user chooses to share and the program will search that drive. TT. 36. The user can then add files to his shared files folder so that anyone on the Internet could download those files. TT. 36. After the user selects his drives, the set-up wizard states "[c]heck the folders you want to be added to your Library. Note that other users cannot add or modify the contents of these folders." Exhibit 5, unnumbered page 20.

A final screen appears to inform the user that the BearShare set-up wizard has been completed. TT. 36. The program also tells the user that some settings have been automatically configured for the user based on the user's internet connection type. TT. 36. The program also tells the user that he may need to review his settings once he's running the program. TT. 36.

As part of the BearShare program, but not as part of the set-up wizard, there are more settings, program options, that can be used to customize the program. TT. 37. These settings are located on the top of the screen. TT. 37. One of the options is "setup." TT. 37. Under "setup" there is searching, uploads, downloads, service, advanced, low power, connection and options. TT. 37.

Under "uploads" a user can choose that he does not want to share any files ever; he only wants to download files. TT. 37-38. This is done by unchecking that box that says "sharing." TT. 38. By default, there is a check in the box that says share files from library. TT. 38. In other words, unless a user unchecks the box, all files he has downloaded will be shared. When a user checks the box in BearShare that says he does do not want to share a

file, the user gets a warning from Bearshare. TT. 44. It says "one of the most valuable contributions you can make to the Gnutella network is to share files. Only when users share files is it possible for everybody or everyone to find the files that they want to download. Please share. Do you want to continue sharing? Yes or no." TT. 44.

So BearShare subscribers do not have to share. TT. 38. BearShare can be operated to share any files or none at all. TT. 36. If a user running BearShare chooses not to share files, he can still use the program to search the Internet for files and download these files; but these files will not be shared. TT. 38.

With BearShare, by default, the folder which is going to be part of a user's shared directory is the "my downloads" folder. TT. 41. That is where files that are downloaded from the Internet would go once they are completely downloaded. TT. 41. A user also can take files that are on CD ROM or any other type of medium and drag and drop them into the shared files folder and they would also be shared. TT. 42.

When a user downloads a file, the Bearshare program lists at the bottom of the computer screen whether or not the file is going to be shared. TT. 43.

Returning to the events on February 28, 2005, the option not to share files via the Bearshare program was available to the defendant on February 28, 2005. TT. 38. The defendant had to have his computer on and be using the "share the files in the library" option on February 28, 2005, when Trooper Erdely did his search because Trooper Erdely found the file being shared and was able to download it from the defendant's computer. TT. 38, 53-54. No one but the defendant lived at 3129 West Queen Lane, Philadelphia, Pennsylvania 19129 on February 28, 2005.

On February 28, 2005, Trooper Erdely knew that there was a movie file that was being shared across the Internet which is named Hindoo. TT. 18. Utilizing the Phex program, he searched the word Hindoo and got a number of hits. TT. 19, 27. Once the result of Trooper Erdely's search came up, the Internet Protocol ("IP") addresses of those sharing the files on which Trooper Erdely got a hit were visible. TT. 19.

One of the IP addresses from one of Trooper Erdely's hits was an IP address belonging to Verizon Internet service. TT. 19. The IP was 141.151.19.66. TT. 19. An IP address is a unique identifier. TT. 19. The file appeared as being shared by this IP address on February 28, 2005 at 4:35 p.m. TT. 19. The complete name of the file being shared by IP 141.151.19.66 was (Hussyfan)(pthc) (r@ygold) (babyshivid) Hindoo4.mpg. Exhibit 5, unnumbered page 2.

Trooper Erdely obtained a state court order compelling Verizon to tell him who was the subscriber with the IP address 141.151.19.66. TT. 20. Verizon informed Trooper Erdely that the subscriber of that service at that date and time was the defendant, Arthur Abraham of 3129 West Queen Lane, Philadelphia, Pennsylvania 19129. TT. 20.

Prior to February 28, 2005, Arthur Abraham was not a name that was known to Trooper Erdely, nor had he ever spoken to or otherwise communicated with the defendant. TT. 20.

Trooper Erdely downloaded the file "Hindoo" that IP address 141.151.19.66 was sharing onto a CD Rom. TT. 21. The file on the CD Rom that Trooper Erdely downloaded from IP address 141.151.19.66 contains child pornography as prohibited by law. TT. 21.

While the subscriber was named as Arthur Abraham, the service address information from Verizon listed one Henry Abraham of 3129 West Queen Lane, Philadelphia,

Pennsylvania 19129. TT. 54. The document with Henry Abraham's name on it was dated

June 3, 2003. TT. 55.

On March 17, 2005, a warrant was obtained to search the defendant's house at 3129

West Queen Lane, Philadelphia, Pennsylvania 19129. TT. 22. Police went to the

defendant's house on March 18, 2005 to search the defendant's house but he was not home.

TT. 23, 62. The police then called the defendant and left him a voice mail message saying

that they wanted to speak to him. TT. 62. The defendant called the authorities back on or

about March 19, 2005 and it was arranged that the police would come to the defendant's

home on March 21, 2005 to talk to the defendant. TT 63. The defendant knew prior to March

21, 2005 that the police wanted to speak to him about a crime. TT. 64.

The troopers arrived at the defendant's residence on the morning of March 21, 2005.

TT. 63. Only the defendant was in the house when the troopers arrived. TT. 64.

Once in the house, troopers asked the defendant if he knew who may have committed

this crime involving child pornography and was he involved. TT. 64. The defendant stated

that he was not involved. TT. 64.

The troopers also asked Mr. Abraham if he had a computer. TT. 64-65. The

defendant responded that he had three computers. TT. 65

The troopers then asked the defendant if he had Internet access to which he replied

that he did. TT. 65. Mr. Abraham then explained that he had Verizon DSL service, but there

had been a problem with his Internet access and it had been turned off. TT. 65. He also said

that he could produce a document concerning the status of his Internet access. TT. 65. The

defendant then went upstairs, accompanied by Trooper Ianace, into a computer-type room

and retrieved from a computer desk a letter from Verizon. TT. 65. The letter from Verizon

said that the defendant had not been paying his bill and explained that if he did not pay the bill, the service would be terminated. TT. 65.

The room where the Verizon letter was found had a computer desk set up. TT. 65. There was a flat screen monitor, a printer and possibly a keyboard and a mouse on the computer desk. TT. 65. Significantly, there was no computer tower. TT. 66. It appeared to Trooper Ianace that the computer tower had been recently moved because there was dust in certain areas and no dust in the area where some of the computer equipment had been removed. TT. 66.

Trooper Ianace asked the defendant what had become of the three computers. TT. 66. Mr. Abraham explained that he had trashed them. TT. 66. He further explained that he had thrown them out in the garbage about a week prior because they were infected with viruses. TT. 66. The defendant could not provide the trooper with an exact date for when he threw the computers out. TT. 66

The troopers also asked the defendant if he lived alone. TT. 66. He said yes, he did live alone. TT. 66. The troopers then asked him how long it had been since he lived with someone in the home or if he had ever lived with anyone in the home. TT. 66. The defendant said he couldn't remember how long it had been since someone had lived in the residence with him. TT. 66.

The troopers asked Mr. Abraham if he would consent to their searching his home; the defendant refused to give consent. TT. 67.

When consent to search the defendant's home was denied, the troopers left the residence with the defendant and got a search warrant which they executed on the same day. TT. 67. Trooper Ianace was one of the authorities who executed the search warrant. TT. 62,

63.

During the search, troopers seized a CD ROM labeled "MISCKV" on the front of the

CD ROM. TT. 23. This CD ROM contained several movie files, one of which was the same

child pornography movie as the file downloaded by Trooper Erdely from the defendant's

computer on February 28, 2005. TT. 23, 48, and 64. The date and time that the relevant

movie image on the MISCKV CD Rom was created was the morning of February 28, 2005.

TT. 48. That is to say that this movie image came into existence on the morning of February

28, 2005 because someone copied it from one location to another, copied it over the Internet

using Gnutella network or copied it from a CD Rom or another piece of medium. TT. 48.

This movie file on the MISCKV CD Rom also had a volume created date of March 19, 2005

at 11:54 a.m. TT. 49. The volume created date is the date the movie file was recorded onto

the CR Rom. TT. 49.

II. The Court's Conclusions of Law.

The Indictment against Defendant charges him with violating 18 U.S.C. § 2252(a)(2).

18 U.S.C. § 2252(a)(2) is entitled "Certain activities relating to material involving the sexual

exploitation of minors," and provides:

> **(a)** Any person who–
>
> **(2)** knowingly receives, or distributes, any visual depiction that has been
> mailed, or has been shipped or transported in interstate or foreign commerce,
> or which contains materials which have been mailed or so shipped or
> transported, by any means including by computer, or knowingly reproduces
> any visual depiction for distribution in interstate or foreign commerce or
> through the mails, if--
>
> **(A)** the producing of such visual depiction involves the use of a minor
> engaging in sexually explicit conduct; and
>
> **(B)** such visual depiction is of such conduct.

18 U.S.C. § 2252(a)(2).

In order for the crime of Distribution of Child Pornography, in violation of Title 18, United States Code, Section 2252(a)(2), to be established, the government must prove all of the following essential elements beyond a reasonable doubt: (1) that the defendant knowingly distributed a visual depiction; (2) that the visual depiction was transported in interstate or foreign commerce or the visual depiction was produced using materials that had been transported in interstate or foreign commerce; (3) that the production of the visual depiction involved the use of a minor engaging in sexually explicit conduct, and portrays that minor engaged in that conduct; and (4) that the defendant knew that the production of the visual depiction involved the use of a minor engaging in sexually explicit conduct, and portrayed a minor engaged in that conduct. Sand, Siffert, Loughlin & Reiss, Modern Federal Jury Instructions, Criminal, Instruction 62-12 (2006).

A. The Government has proven beyond a reasonable doubt that the Defendant distributed a visual depiction.

First, the Government has proven beyond a reasonable doubt that the Defendant distributed a visual depiction on February 28, 2005 when the Defendant used the Bearshare file-sharing program to make the movie image at issue available to other users on the Gnutella network and Trooper Erdely was able to download the movie image from the defendant's computer to his computer.

Given that this issue is one of first impression, we take the time to explain our interpretation of the terms "distribute" and "distribution" in 18 U.S.C. § 2552(a)(2).

We interpreted the terms "distribute" and "distribution" in 18 U.S.C. § 2552(a)(2) using standard principles of statutory construction. Thus, as explained in In re Armstrong

World Industries, Inc., 432 F.3d 507 (3d Cir. 2005):"[w]e beg[a]n by looking at the plain language of the statute. See United States v. Ron Pair Enterprises, Inc., 489 U.S. 235, 241, 109 S.Ct. 1026, 103 L.Ed.2d 290 (1989). If the meaning is plain, we make no further inquiry unless the literal application of the statute will end in a result that conflicts with Congress's intentions. Id. at 242-43, 109 S.Ct. 1026. In such a case, the intentions of Congress will control." Id. at 512. Significant in this case since the terms "distribute" and "distribution" are not defined in the statute, when there is no indication that Congress intended a specific legal meaning for a term, the court may look to sources such as dictionaries for a definition. See Muscarello v. United States, 524 U.S. 125, 118 S.Ct. 1911, 1914-16 (1998) (Court relied, in addition to legislative history, on dictionaries, literature and newspaper reports to ascertain the meaning of "carry").

Thus, turning to 18 U.S.C. § 2252, and applying the above rules of statutory interpretation, we looked first at the plain language of 18 U.S.C. § 2252. Notably, the terms "distribute" and "distribution" are not defined in the 18 U.S.C. § 2252 and there is no indication that Congress intended a specific legal meaning for the term "distribute" and "distribution." Therefore, we looked at the ordinary meaning of these terms. Black's Law Dictionary defines "distribution" as "2. The act or process of apportioning or giving out" and defines "distribute" as "1. To apportion; to divide among several; 2. To arrange by class or order. 3. To deliver. 4. To spread out; to disperse." Black's Law Dictionary (8th ed. 2005). The word "disperse" is defined as "to spread or distribute from a fixed or constant source; disseminate." Merriam Webster Collegiate Dictionary (2005)

Next we examined the plain language of the statute in light of Congress's intentions in enacting 18 U.S.C. § 2552. Congress's intent in enacting 18 U.S.C. § 2252 was a broad

one, to protect children from sexual exploitation. See S.Rep. No. 438, 95th Cong., 2d Sess. 3,

reprinted in 1978 U.S.C.C.A.N. 40, 41. See also United States v. Mohrbacher, 182 F.3d

1041, 1049 (9th Cir. 1999) (explaining that the statutory provisions of 18 U.S.C. § 2252

"must be interpreted in accord with the statute's broad and general purpose of facilitating the

prosecution of individuals who are involved with child pornography"). Interpreting the terms

in question by their plain meaning, i.e. "distribute" means to deliver or disperse and

"distribution" means the act of delivering or dispersing, does not end in a result that conflicts

with Congress's intent in enacting 18 U.S.C. § 2252 to protect children from sexual

exploitation.

Therefore, we interpreted "distribute" to mean to deliver or disperse and

"distribution" to mean the act of delivering or dispersing, and applied this interpretation to

the facts of this case. Having done so, we find that the defendant distributed a visual

depiction when as a result of the defendant's installation of an internet peer-to-peer video file

sharing program on his computer, a Pennsylvania state trooper was able to download the

child pornography from the defendant's computer to the trooper's computer.

B. The Government has proven beyond a reasonable doubt that the Defendant's

distribution of the visual depiction was done knowingly.

An act is done knowingly when it is done voluntarily and intentionally and not

because of accident, mistake or some other innocent reason. The Court finds that the

Government has proven beyond a reasonable doubt that the Defendant knowingly distributed

the movie image in question. The Defendant chose to share the movie image in question with

anyone using the Gnutella network via the Bearshare file-sharing program which he installed

on his computer. His act of choosing to share the movie image was voluntary on his part. He

did not have to share the movie image; the Bearshare program allowed him the option not to share any file he downloaded. Neither the fact that the Defendant did not personally know Trooper Erderly nor the fact that Trooper Erderly had not had any communication with the defendant prior to downloading the chid pornography is relevant.

C. The Government has proven beyond a reasonable doubt that the visual depiction was shipped or transported in interstate or foreign commerce or the visual depiction was produced using materials that had been transported in interstate or foreign commerce.

The Government also has proven beyond a reasonable doubt that the visual depiction was shipped or transported in interstate or foreign commerce or the visual depiction was produced using materials that had been transported in interstate or foreign commerce. The transmission of the movie image in question by computer over the Internet via the Gnutella network through the use of a peer-to-peer file sharing program constitutes transportation in interstate commerce.

D. The Government has proven beyond a reasonable doubt that the production of the visual depiction involved the use of a minor engaging in sexually explicit conduct, and portrays that minor engaged in that conduct.

The Government has established beyond a reasonable doubt the production of the visual depiction involved the use of a minor engaging in sexually explicit conduct, and portrays that minor engaged in that conduct. The parties stipulated that "[t]he video contained on Government Exhibit #1 depicts a minor engaged in sexually explicit conduct." Stipulation of Fact and Authenticity, ¶ 3. Additionally, the Court was able to see for itself, from its brief
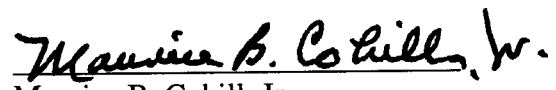
viewing of Exhibits 1 and 2, that the production of the visual depiction involved the use of a minor engaging in sexually explicit conduct, and portrays that minor engaged in that conduct.

E. The Government has proven beyond a reasonable doubt that the Defendant knew that the production of the visual depiction involved the use of a minor engaging in sexually explicit conduct.

"[T]he term 'knowingly' in § 2252 extends both to the sexually explicit nature of the material and to the age of the performers." United States v. X-Citement Video, Inc., 513 U.S. 64, 78, 115 S.Ct. 464, 472 (1994). "To fulfill the knowledge element of § 2252, a defendant simply must be aware of the general nature and character of the material . . . . " United States v. Knox, 32 F.3d 733, 754 (3d Cir. 1994), cert. den'd, 513 U.S. 1109, 115 S.Ct. 897 (1995). We find that the Government has proven beyond a reasonable doubt that the defendant knew that the production of the visual depiction involved the use of a minor engaging in sexually explicit conduct, and portrayed a minor engaged in that conduct. This element was proven beyond a reasonable doubt by a combination of a number of pieces of evidence, including the defendant telling Trooper Ianace that he had disposed of his hard drive in the trash because of a "virus" around the same time the defendant had been told by the police that they wanted to speak to him as part of a criminal investigation, and that the defendant possessed a CD ROM labeled "MISCKV" that had on it a movie image that was the same as the movie image downloaded by Trooper Erdely from the Defendant's computer. Justice Potter Stewart so aptly stated in his concurring opinion in Jacobellis v. State of Ohio, 378 U.S. 184, 197 (1964): "I know it when I see it . . . ."

III. Conclusion.

The Government having proven beyond a reasonable doubt that Defendant Arthur Abraham violated all the essential elements of 18 U.S.C. § 2252(a)(2), the Court finds the defendant is guilty of violating 18 U.S.C. § 2252(a)(2) and a judgment of guilty shall be entered as to Count 1 of the Indictment against Defendant Arthur Abraham.

Maurice B. Cohill, Jr.

Maurice B. Cohill, Jr.
Senior United States District Judge

Dated: October 19, 2006